Treasury Inspector General for Tax Administration

EMPLOYEES CONTINUE TO BE SUSCEPTIBLE TO SOCIAL ENGINEERING ATTEMPTS THAT COULD BE USED BY HACKERS

Issued on July 20, 2007

Highlights

Highlights of Report Number: 2007-20-107 to the Internal Revenue Service Chief, Mission Assurance and Security Services.

IMPACT ON TAXPAYERS

The Internal Revenue Service (IRS) has nearly 100,000 employees and contractors who have access to tax return information processed on approximately 240 computer systems and over 1,500 databases. Using social engineering tactics, TIGTA determined IRS employees, including managers, are not complying with the rudimentary computer security practices of protecting their passwords. As a result, the IRS is at risk of providing unauthorized persons access to taxpayer data that could be used for identity theft and other fraudulent schemes.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of our statutory requirements to annually review the adequacy and security of IRS technology. The overall objective of this review was to evaluate the susceptibility of IRS employees to social engineering attempts that could be used by hackers to gain access to IRS systems.

WHAT TIGTA FOUND

IRS employees continue to struggle with complying with the basic security requirements of protecting their passwords and reporting possible security incidents. TIGTA made 102 telephone calls to IRS employees, including managers and a contractor, and posed as a helpdesk representative seeking assistance to correct a network problem. Under this scenario, TIGTA asked the employee to provide his or her username and temporarily change his or her password to one TIGTA suggested. TIGTA was able to convince 61 (60 percent) of the 102 employees to comply with the request. Some of the notable reasons given were that the employee thought the scenario sounded legitimate and believable, did not think changing his or her password was the same as disclosing the password, or had experienced past computer problems.

TIGTA had conducted similar social engineering test telephone calls in August 2001 and December 2004, which yielded 71 percent and 35 percent noncompliance rates, respectively. In response to the two audits, the IRS took corrective actions to raise awareness over password protection requirements and social engineering attempts. However, the correction actions have not been effective. Based on the results of this audit, TIGTA concluded employees either do not fully understand security requirements or do not place a sufficiently high priority on protecting taxpayer data in their day-to-day work.

In addition, only 8 of the 102 employees contacted the TIGTA Office of Investigations or the IRS computer security organization to validate whether the test was an official TIGTA audit.

WHAT TIGTA RECOMMENDED

TIGTA recommended the Chief, Mission Assurance and Security Services, continue security awareness activities to remind employees of the potential for social engineering attempts and the need to report these incidents to the IRS computer security organization, conduct internal social engineering tests on a periodic basis to increase employees' security awareness and the need to protect usernames and passwords, and coordinate with business units to emphasize the need to discipline employees for security violations resulting from negligence or carelessness.

In their response to the report, IRS officials stated the Mission Assurance and Security Services organization plans to continue to deliver social engineering messages and use results from a social engineering survey to remind employees of the potential for social engineering attempts and the need to report these incidents to the IRS Computer Security Incident Response Center. The IRS plans to conduct at least one internal social engineering test during Fiscal Year 2008 to increase employees' security awareness and the need to protect usernames and passwords. The test will be robust and statistically diverse, surveying thousands of IRS employees. The IRS plans to communicate the test results to business units to increase awareness. Additionally, a revised Penalty Guide has been developed and is currently being negotiated with the National Treasury Employees Union. When the Guide is published, the IRS plans to emphasize to the business units the need to implement the new guidance.

READ THE FULL REPORT

To view the report, including the scope, methodology, and full IRS response, go to:

http://www.treas.gov/tigta/auditreports/2007reports/200720107fr.pdf.

Email Address: Bonnie.Heald@tigta.treas.gov
Phone Number: 202-927-7037
Web Site: http://www.tigta.gov